Storing Our Lives Online: Expanded Email Storage Raises Complex Policy Issues

ARI SCHWARTZ, DEIRDRE MULLIGAN, & INDRANI MONDAL*[1]

ABSTRACT

ISPs and other email service providers are increasingly offering their customers the ability to store, on the service providers' computers, very large quantities of information. This free or low cost storage offers Internet users the convenience of access to their email and attached documents and photographs from any Internet-connected computer in the world. However, it also has unintended consequences for personal privacy, especially because privacy laws were written when consumer use of such remote storage was rare.

For this paper, we reviewed existing legislation governing stored electronic communications and data, and we examined the storage practices and disclosure policies of some of the most well-known ISPs.

We found that online service providers address many privacy issues associated with storage through their terms of service and privacy policies. For the most part, leading service providers promise consumers relatively strong protections and adhere to them. However, it is sometimes hard to determine what a specific provider's policy is, especially with respect to deletion of mail from inactive accounts or deletion of older mail from active accounts. When it comes to government access, the best privacy policy in the world yields to a warrant or perhaps even a mere subpoena, often without notice to the customer that her personal documents are being disclosed. Since ISPs retain data for varying lengths of time, and do not always delete email immediately upon

---

* Ari Schwartz is an Associate Director of the Center for Democracy and Technology (CDT). His work focuses on increasing individual control over personal and public information. Prior to working at CDT, Ari worked at OMB Watch researching and analyzing the nonprofit sector's engagement in technology, government performance, access to government information, and government information technology policy.

Deirdre K. Mulligan is the director of the Samuelson Law, Technology & Public Policy Clinic and an acting clinical professor of law at the UC Berkeley School of Law (Boalt Hall). Before coming to Boalt, she was staff counsel at the Center for Democracy & Technology in Washington.

Indrani Mondal worked on this publication during an internship at the Center for Democracy and Technology. She will be pursuing a Masters in Public Policy and Management at the Heinz School at Carnegie Mellon University beginning fall 2005, her focus will be on information technology policy.

[1] The authors would like to thank James Dempsey and Lara Flint for their detailed input.

request, customers may not even be aware of whether their email is still stored, and thus susceptible to disclosure.

Most importantly, we found that the major law setting rules for government access to email, the Electronic Communications Privacy Act of 1986 (ECPA), no longer offers adequate privacy protections, given changes in the way people today use their email accounts and remote storage. We conclude that, given the rapid onset of the storage revolution, consumer expectations are likely out of line with the realities of online privacy protection. In the new environment of massive storage capacity, reform is needed on both the government side and the industry side. The best approach to dealing with the policy issues posed by increased online storage is a mix of consumer education, clear ISP policies, and updates to ECPA and other pertinent privacy laws.

INTRODUCTION

Internet Service Providers (ISPs) and Web-based providers of email are offering consumers free email with expansive storage and searching capability. Additional services include Web-posting and online calendars that enable information sharing with friends and colleagues. These services provide storage space that was unimaginable twenty years ago.

While these services offer consumers flexibility and mobile access, they raise a range of concerns because they reflect a sea of change from the concepts on which the legal framework for electronic communications was originally based. These concerns include:

> the diminishing relevance of traditional constitutional search and seizure rules, combined with the limitations of statutory privacy protections, as information moves out of the home, off personal computer hard drives, and onto remote servers;
>
> some lack of transparency and clarity regarding ISP practices in storing or deleting subscriber emails;
>
> the legal uncertainty surrounding what ISPs can do with the personal information and communications of their customers; and
>
> the difficulty next of kin may encounter in retrieving important information held in a deceased user's account.

This paper will offer recommendations for legal reforms and improved best practices.

THE STORAGE REVOLUTION

As the Internet has moved into schools, homes, and offices, email has become a primary means of communication, and the Web has become an important means of storing and retrieving information. While the telephone is still a more ubiquitous medium, email and other internet communications are often cheaper and are used more often than the telephone or traditional mail for certain kinds of transactions. Unlike telephone calls, emails can be easily saved for future reference. Moreover, unlike telephone calls and traditional mail, copies of email can be stored with the service provider. Until recently, this potential of third party storage was largely unrealized; the primary means of storing older email was on one's desktop computer after download. Due in part to cost considerations, providers of free services used to offer their customers the ability to store only a relatively small amount of email on the service provider's computer.

However, innovations in storage technology have enabled the retention of much larger amounts of data at lower costs. As the National Institute for Standards and Technology has pointed out, the nation's digital storage industry – makers of the tapes, disks, and other gear that have become the archives and the retrieval tools of the information age – has been doubling storage capacity about every 18 months.[2] The first hard disk drive produced by IBM in 1956 had a capacity of 5 megabytes. In 1998, the IBM Deskstar hard drive had a 25-gigabyte capacity, which is approximately 5000 times the capacity of the first drive. One year later, IBM announced the 73-gigabyte hard drive.[3] According to one industry estimate, 1 gigabyte worth of magnetic disk storage capacity cost $8.37 in 2000 and is expected to cost $0.42 by 2005 and less than a penny by 2013.[4]

---

[2] Advanced Technology Forum, National Institute of Standards and Technology, Digital Data Storage, available at http://www.atp.nist.gov/atp/focus/dds.htm (last accessed May 25, 2005).

[3] Fortune City, Storage Devices, at http://www.fortunecity.com/marina/reach/435/storage.html (last visited Mar. 10, 2005).

[4] Steve Gilheany, The Decline of Magnetic Disk Storage Cost Over the Next 25 Years, available at http://www.berghell.com/whitepapers/Storage%20Costs.pdf (last visited Mar. 10, 2005).

In April 2004, Google started to beta-test its "Gmail" system, which provides users with 1 gigabyte of storage space for free. This represented 500 times the amount of the equivalent MSN/Hotmail account at the time.[5] In response to the "Gmail" offering, Yahoo! announced that it would increase free customer storage space to 100 megabytes and that paid customers would receive 2 gigabytes. MSN/Hotmail followed, declaring that it would upgrade the storage space of free accounts to 250 megabytes and paid accounts to 2 gigabytes. Then a year later, Google upped the ante, by providing 2 gigabytes for free to Gmail beta-testers.

This dramatic growth in storage capacity comes at a time when more email is being read via webmail accounts. In the past, particularly at the time when current email privacy laws were written, email users accessed their email by downloading it onto their personal computers. Now, email – including email that has been read but which still has value to the user – often sits on a third party server accessible via the Web.

In addition, various other consumer technology developments drive the demand for greater storage space. For example, the combination of digital cameras and higher bandwidth connections encourages users not only to send photographs as email attachments but also to store photos on personal Web spaces offered on the systems of service providers. Online merchants encourage customers to create online itineraries or profiles, storing historical records on service providers' computers for easy access from any Internet-connected computer. Confirmations of online airline ticket purchases come through email, creating a record of the travel that may also reside with the email service provider.

As one analyst for Jupiter Research stated, "[t]he key thing about increasing storage is to make the e-mail service more of a core resource in the user's computing life. If you can put 250 megabytes worth the consumer will use it more often."[6] Further encouraging increased usage, email providers are emphasizing complementary services, such as searching capabilities, photo albums and file servers. As Google asks its Gmail users, "Who needs to delete when you have

---

[5] Hiawatha Bray, *Google's Gmail Is Still a Rough Draft*, BOSTON GLOBE, May 31, 2004, *available at* http://www.boston.com/business/technology/articles/2004/05/31/googles_gmail_is_still_a_rough_draft/ (last accessed Apr. 23, 2005).

[6] Janis Mara, MSN Hotmail Upgrades E-Mail, Increases Storage, ClickZ News, June 24, 2004, at http://www.clickz.com/news/article.php/3372781 (last accessed Apr. 23, 2005).

1000 MB of storage?!"[7] With the changes presaged by Gmail, it is clear that consumers will be storing more mail and attachments on third party servers.

While the technology offers a welcome set of new services for consumers, most users are not aware of the consequences that flow from the decision to store their personal information and files remotely. Unless the law catches up, loss of privacy may be a hidden and unintended price of these new services. Under current law, a consumer's personal communications and records in electronic storage with an ISP or other service provider are afforded less privacy than those same communications in transit, and less than if they were stored on the consumer's own computer or printed out and put in a physical file cabinet. Consumers are not aware of these legal distinctions and have little or no idea what kind of access government agents have to their stored data. Similarly, consumers probably do not know what use ISPs can make of their stored email and files. For all these reasons, it is likely that the rules controlling government and ISP access to these personal records are inconsistent with consumers' privacy expectations.

THE CURRENT RULES FOR GOVERNMENT ACCESS

The Fourth Amendment to the U.S. Constitution shields individuals from unreasonable government searches and seizures. The Supreme Court has said that the Fourth Amendment protects "people, not places."[8] Under the Court's analysis, whether a search violates the Fourth Amendment turns on whether the individual has a "reasonable expectation of privacy." This is a two-part inquiry that asks first whether the individual's conduct reflects "an actual [subjective] expectation of privacy" and, if the answer is yes, whether that expectation is "one that society [objectively] is prepared to recognize as 'reasonable.'"[9] Under this analysis, the Supreme Court has held that the Fourth Amendment protects not only a person's home or apartment and his physical person, but also the content of his telephone calls. While the Court has never explicitly ruled on email, it

---

[7] This is the message that Gmail users receive when they look in their trash folder if nothing has been deleted. In its entirety, the message reads: "No conversations in the trash. Who needs to delete when you have 1000 MB of storage?!"

[8] Katz v. United States, 389 U.S. 347, 351 (1967).

[9] *Id.* at 360-61 (Harlan, J., concurring).

has been assumed that the same Fourth Amendment protection would apply to email in transit.

However, in a series of cases in the 1970s, the Supreme Court held that the Fourth Amendment does not apply to personal information contained in records held by third parties. Once an individual voluntarily discloses information to a business, the Court reasoned, the individual no longer has a reasonable expectation of privacy in the data and the government can access the record without raising any constitutional privacy concerns.[10]

Although these "business record" decisions predated the digital revolution, they are still cited to support the proposition that individuals have no constitutionally protected privacy interest in personal information and records voluntarily disclosed to businesses. Under this theory, everything from medical records at hospitals and insurance companies, to copies of cancelled checks held by banks, to records of who calls whom compiled by telephone companies, fall outside the Constitution. Unless these records are protected by statute (which some business records are), they can be freely disclosed by service providers to the government and to others.

> There are serious questions whether the business records doctrine is still constitutionally sound, given the revealing nature of the huge amounts of transactional data generated by electronic systems today. Moreover, it has never been clear whether the business records doctrine properly applies to the content of stored communications. The business records doctrine was developed when courts did not foresee the ability of a communications service provider to store the content of communications. Nor did courts anticipate the role of the Internet in decentralizing data storage outside the

---

[10] In *Couch v. United States*, 409 U.S. 322 (1973), the Court held that subpoenaing an accountant for records provided by a client for the purposes of preparing a tax return raised neither Fifth nor Fourth Amendment concerns. In *United States v. Miller,* 425 U.S. 435 (1976), the Court held that records of an individual's financial transactions held by his bank were outside the protection of the Fourth Amendment. Lastly, in *Smith v. Maryland,* 442 U.S. 735 (1979), the Court held that individuals have no legitimate expectation of privacy in the phone numbers they dial, and therefore the installation of a technical device (a pen register) that captured such numbers on the phone company's property did not constitute a search. *See generally*, Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. Rev. 1557 (2004); *see generally* James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, 8 ALB. L.J. SCI. & TECH. 65 (1997).

> home or office. The doctrine does not take into account case law that limits government access to items held by a third party in physical storage, such as a storage locker. When an individual stores personal property with a third party, the owner of the property often retains a privacy interest in the stored items, meaning that a warrant would be required to search the storage space. Under that analogy, transactional information regarding the terms of storage might not be protected by the Fourth Amendment, but the stored items themselves – in this case, the contents of stored email – might be.[11]

It is time to reconsider the limits of the business records doctrine as applied to Internet communications and stored documents, for the doctrine has played an important role in shaping the privacy protections currently applied to email and other records when they are in storage with a service provider.[12]

In 1986 Congress adopted the Electronic Communications Privacy Act (ECPA). ECPA set rules for real-time interception of electronic communications, requiring a special warrant for access to email in transit just as had been required for tapping voice communications; restricted law enforcement access to transactional information in real-time with the Pen Register/Trap and Trace statute; and adopted rules on access to stored electronic communications and stored transactional records held by service providers.[13]

The part of ECPA addressing stored communications, known as the Stored Communications Act (SCA), set rules for the government to obtain the content of stored emails, transactional information related to emails such as the senders and recipients, and subscriber identifying information about the users of email services. In many ways, ECPA was a remarkable law, but some of the distinctions in the SCA that made sense in 1986 no longer seem valid. The rules are complex, drawing many fine distinctions about which users are probably completely unaware and that no longer match patterns of Internet

---

[11] For a discussion of storage cases and more on the applicability of this concept to stored communications, see Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 Geo. Wash. L. Rev. 1375, 1405-06 & nn.185-86 (2004).

[12] This process of reexamination has begun. *See id.*; *see* Mulligan, *supra* note 10.

[13] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986), *available at* http://nsi.org/Library/Comm/ecpa.txt.

usage.[14] Influenced in part by the business records doctrine (even though, as noted above, it has never been clear that the doctrine should apply to the content of stored communications), ECPA's standards for government access to email messages vary depending on whether the email is "in transit" or resting in storage on the server of the recipient's ISP. If the email is in transit, it is entitled to the highest protection under the wiretap law.[15] Stored email is entitled to less protection, and the level of protection depends on how long it has been stored and possibly on whether it has been "opened" or not. In general, email stored with a service provider for 180 days or less is afforded full Fourth Amendment protection (although not the higher protection of the wiretap laws) and can be disclosed to the government only pursuant to a warrant issued on the basis of probable cause.[16] Email stored on the server of an ISP or other service provider for more than 180 days can be disclosed pursuant to a court order or even a mere subpoena at a much lower standard.[17] And the Department of Justice maintains that even very recent email stored on the computer of a service provider falls under the lower standard of protection as soon as it is opened by the customer.[18] To date, the only federal appellate court to consider this issue rejected the government's position, finding that within the 180-day period opened and unopened messages enjoy

---

[14] Mulligan, supra note 10; Orin S. Kerr, A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It, 72 GEO. WASH. L. Rev. 1208 (2004).

[15] Government must have a court order issued on probable cause to intercept email messages in transit. 18 U.S.C. § 2518 (2002).

[16] Governmental entities are required to use a warrant to access the contents of electronic communications in "electronic storage" for 180 days or less. 18 U.S.C. § 2703(a).

[17] If electronic communications are older than 180 days, the government may compel disclosure using a variety of less protective instruments, including a warrant executable without notice to the subscriber or a subpoena with notice or delayed notice. 18 U.S.C. § 2703(b).

[18] The government's position is that if a message is opened but remains on an ISP's server, it is no longer subject to search warrant requirements under the Stored Communications Act because it is not in "electronic storage" (defined as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an electronic communication service for purposes of backup protection of such communication," 18 U.S.C. § 2510(17) (2002)), which is the statutory test for full protection. Instead, the opened email is merely being held for storage purposes and is therefore accessible under the lower standards of 18 U.S.C. § 2703(b) (2002).

uniform privacy protections.[19] Disclosures to government entities by cable ISPs are governed by the same rules.[20]

The SCA also draws a distinction between providers of "electronic communication services," which give consumers the ability to send and receive email, and "remote computing services," which store or process their customer's data. Under ECPA, the content of records held by remote computing services can be accessed by the government with a mere subpoena. Many ISPs today are both electronic communication services and remote computing services. The ECPA drafters had in mind the 1980s model of email services: users would download email off the service provider's computer and generally did not leave their email in the hands of the service provider. Today, many mail programs are accessed through World Wide Web interfaces, so email is by default stored on Web servers of third parties.

As a result of these complex rules, the same email message will be subject to many different rules during its life span. These rules likely do not match the expectations of email users. Most users are not aware, for example, that stored email loses some privacy protection when it is more than 180 days old or that even a new email may be entitled to less privacy protection as soon as it is opened.

A June 2004 decision by the federal appeals court in Boston triggered a controversy that illustrated another way in which ECPA does not match user expectations. The case, *United States v. Councilman*,[21] noted that an ISP could read and use for its own business purposes (but not disclose to others) the emails of subscribers held in storage on the service provider's computers. The court went one step further and held that emails could be read by service providers even when they were in the very brief temporary storage that occurs as an email is being transmitted. Mainstream ISPs do not read their customers' email – the small ISP at issue may have been unique – but the case drew attention to an overlooked gap in the law and led to a rare *en banc* rehearing of the case.[22] Many in industry feel that, given

---

[19] The Ninth Circuit found that the Stored Communications Act covers electronic messages received and opened by a recipient and resting on the service provider's servers because they were "stored . . . for purposes of backup protection." Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2004), *cert. denied*, 73 U.S.L.W. 3206 (U.S. Oct. 4, 2004) (No. 03-1565).

[20] *See* 47 U.S.C. § 551(c)(2)(D) (2001), added by § 211 of U.S. Patriot Act in 2001.

[21] United States v. Councilman, 373 F.3d 197 (1st Cir. 2004), *reh'g en banc granted*, 385 F.3d 793 (1st Cir. 2004).

[22] *See* CDT Policy Post 10.13, *Email Privacy Protection Called into Question by Federal Appeals Court Decision* (July 30, 2004), *at* http://www.cdt.org/publications/pp_10.13.shtml

the practices of legitimate ISPs, the *Councilman* controversy is overblown. ECPA's failure to prohibit ISPs from reading their subscribers' email, however, is in contrast to the law governing telephone companies, which does prohibit them from listening to customer conversations except to ensure service quality, detect fraud, or otherwise provide service.[23]

CIVIL SUBPOENAS

The use of civil subpoenas to obtain information from ISPs has recently received greater media attention, in part due to the recording industry's initiative to subpoena the ISP records of individuals who are accused of sharing copyrighted music files. For years, however, civil subpoenas have been served on ISPs in civil disputes such as divorce or custody cases, employment litigation, defamation, and other cases between private parties.

ECPA focuses on government surveillance concerns, and it offers no clear guidance on access to records by private litigants. ECPA generally prohibits disclosures of the contents of stored email to private parties, with certain exceptions.[24] None of the exceptions expressly authorizes disclosures to private parties pursuant to a civil subpoena. On the other hand, ECPA provides that ISPs can disclose any records pertaining to subscribers other than the content of communications to private parties without the subscriber's permission and without a subpoena.[25] (It is important to note that, as a matter of policy, many ISPs do not disclose subscriber information without a subpoena. To the extent that this policy is stated in a privacy policy or terms of service, it is legally binding.) In addition, there is no requirement in ECPA that the service provider disclosing records or

---

(last accessed Apr. 23, 2005). CDT filed an amicus brief urging reversal (siding with the Justice Department). The *en banc* review pertains only to the question of whether emails can be read while in temporary storage incident to transmission. An en banc reversal will probably leave untouched the rule that ISPs can read their customers' emails after they come to rest in the recipient's inbox on the ISP's server. That rule, even though it seems inconsistent with Congress' overall intent in ECPA, does seem to be statutorily based, so its revision will require legislative action. The court's *en banc* decision is expected sometime in 2005.

[23] 18 U.S.C. § 2511(2)(a)(i) (2002).

[24] 18 U.S.C. § 2702 (2003).

[25] 18 U.S.C. § 2702(c)(6) (permitting disclosure of subscriber information (not including the contents of communications) to "any person other than a governmental entity").

email content to a private litigant, or the private litigant obtaining them via subpoena give any notice to the person whose information is being sought.[26] In contrast, the Cable Act, unlike ECPA, does expressly address the question of private party access to the content of stored email. If the ISP is covered by the Cable Act, that law requires parties in civil suits to obtain a court order and requires the cable operator (offering ISP service in this instance) to provide notice to the subscriber.[27]

The process surrounding civil subpoenas can be complicated. For example, a lawsuit may be filed in New York, the service provider upon whom the subpoena is served may be in Virginia, and the individual whose information is sought may live in California. Even if a subpoena is issued by a court in the same state as the user's ISP and the user is notified of the subpoena, the notice may not direct him to the court in which the lawsuit is being filed or provide information about the claims being made. To respond, even an individual who realizes that her information has been requested would probably need to hire a lawyer in the state where the subpoena is served or the state where it was issued, or both, in order to file a formal objection prior to the information being released by the service provider.

DELETION FROM STORAGE

Even as service providers offer expanded storage capacity, many have tightened their rules for how long they will store information in unused accounts before terminating the account and deleting the email. This is understandable from a business perspective, because providers want to purge unused accounts in order to free up more space for those actually using it. However, users may not read the fine print and may be astonished to find that information left in an unused account has been wiped out, particularly if it was deleted without specific warning.

---

[26] Virginia has a law requiring notification of ISP customers of a civil subpoena prior to disclosure. *See* VA. CODE ANN. § 8.01-407.1(A)(3) (2004), *available at* http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+8.01-407.1 (last accessed Apr. 23, 2005). A similar proposal was before the California legislature but was not adopted. *See* The Internet Communications Protection Act, A.B. 1143, 2003 Legis. Reg. Sess. (Cal. 2003), *available at* http://www.leginfo.ca.gov/pub/03-04/bill/asm/ab_1101-1150/ab_1143_bill_20040621_amended_sen.html (last accessed Apr. 23, 2005).

[27] Cable Act, 47 U.S.C. § 551(c)(2)(B) (2001) (as amended by the Patriot Act to make it clear that, when a cable company is acting as an ISP, it is covered by ECPA for purposes of disclosures to government entities, but the Patriot Act did not change the rules for cable ISP disclosures to private parties in civil litigation.).

A second question concerning deletion is when the provider will automatically delete older mail from a still active account. It is appropriate that policies differ from provider to provider – certainly Google's competitive offer of a service that never deletes email expands consumer choice – but there is a question whether users are adequately informed of other ISPs' policies.

A third issue is whether records "deleted" by the subscriber are actually removed from all backup storage. Actual practice may not match the ordinary user's expectation that if he cannot retrieve a message himself, then it cannot be retrieved at all. Google's Gmail privacy policy raises an interesting point about "deletion time." Google notes that it cannot assure that all backups of information will be deleted immediately when a user requests that information be deleted. In speaking with Google representatives about this issue, they say that they are actually following industry practices, but feel compelled to advise users that it is impossible to promise that all deletion requests will be immediately implemented throughout their system. Google says that information that a user believes to have been deleted could be still available when a subpoena is issued.[28]

NEXT OF KIN REQUESTS

Access can also be a concern for family members who want access to the account of a relative who has died. Much of an individual's personal business may have been conducted through email, and surviving next of kin may want to gain prompt access to that information. While service providers often would like to help families, security and privacy concerns put the service providers in a difficult situation; at the least, service providers want to be sure they are dealing with the legitimate heirs or executors of a deceased customer before releasing what may be sensitive and even valuable information.[29] Given that email accounts are typically not shared with others, they may contain communications that the deceased, if given the option, would not choose to provide to relatives. As people store more information with third parties, these dilemmas will continue to

---

[28] While some ISPs claim to delete instantly, they are probably not overwriting the information instantly, leaving it available for discovery by forensic experts. Google is careful not to claim that information is instantly deleted if it could possibly be made available during discovery.

[29] Jeffrey Selingo, *Whose Data Is It, Anyway?*, N.Y. TIMES, June 3, 2004, at G1.

grow.[30] It is unclear whether the resolution of the issues lies solely in privacy law or will be best dealt with in combination with property and estates law.

STUDY OF INDUSTRY PRACTICES

During the summer of 2004, the Center for Democracy and Technology conducted a study of industry practices in relation to data storage and access. We examined the policies of seven of the largest commercial email providers. We collected most of our information from the providers' Web sites, including terms of service and privacy policies. When we could not find information, we called the ISPs' help lines. We shared a draft of the results with the chief privacy officer or legal counsel for each of the service providers studied.

Our survey covered five issues:

> (1) Deletion Without Subscriber Request – When is an inactive account terminated and its contents deleted, and when is email automatically deleted from an active account?
>
> (2) Deletion upon Request – How long does it take to remove mail from the provider's server after the user deletes it from her screen?
>
> (3) Next of Kin Access – What documentation is required from relatives in order to provide access to next of kin records?
>
> (4) Civil Subpoenas – Do email service providers give notice to a subscriber whose records are sought pursuant to a civil subpoena?

---

[30] The issue is complex. Stored email implicates the privacy not only of the account holder but also of those who corresponded with the account holder. The issue was illustrated recently when Yahoo! denied the father of a U.S. Marine killed in Iraq access to the son's Yahoo email account. The company felt bound by its terms of service, in which the company promises not to disclose private email communications of its users. Our research indicated that Yahoo's policy is to never transfer email, but a news story indicated that Yahoo! Would disclose the stored data if family members obtained a court document verifying their identity and relationship with the deceased. Jim Hu, *Yahoo Denies Family Access to Dead Marine's E-mail*, CNET NEWS.COM, Dec. 21, 2004, *at* http://news.com.com/Yahoo+denies+family+access+to+dead+marines+e-mail/2100-1038_3-5500057.html (last accessed Apr. 23, 2005).

(5) Reading Customer Email – Do the privacy notice and terms of service agreement explicitly state that the company does not read its customers' emails for purposes other than providing service, enforcing terms of service, or protecting the rights of the ISP?

We studied the practices only of the larger email providers. Smaller ISPs may not have set policies on these matters.

The following chart summarizes the results of our survey. It turned out that even from the large ISPs, it was sometimes difficult to track down the policies addressing our questions, which suggests that companies need to be more conscious of these issues and need to inform users in a clear manner. The information below is accurate to the best of our ability. We regret any errors.

	Automatic Deletion – When is an inactive account terminated and when is email deleted from an active account?	Deletion Upon Request – Number of days between date deleted by subscriber and date removed from server.	Next of Kin Access – What is required to gain access to the email of a deceased relative?	Civil Subpoenas – Is notice given to subscriber whose information is sought? When is the information handed over? *	Stated Policy Against Reading Subscriber Email**
MSN/ Hotmail Free	Termination - 30 days from date of last activity Automatic deletion - Sent email → automatically deleted every 30 days	3 days	Show death certificate and official proof that you are next of kin	Notify subscriber whose information is being sought Release information after 2 weeks	Implies no
MSN/ Hotmail Paid	Termination - General account is closed 30 days from date of missed payment Automatic deletion - Junk email → automatically removed every 7 days	3 days	Provide credit card number that the account is registered under to transfer account	Notify subscriber whose information is being sought. Release information after 2 weeks	Implies no
Google Gmail[31]	Termination - 90 days from last activity Automatic deletion – never	Unspecified (eventually will be deleted/ overwritten)	Under review (have not had any requests to date)	Notify member whose information is being sought. Release information after 20 days	Unclear

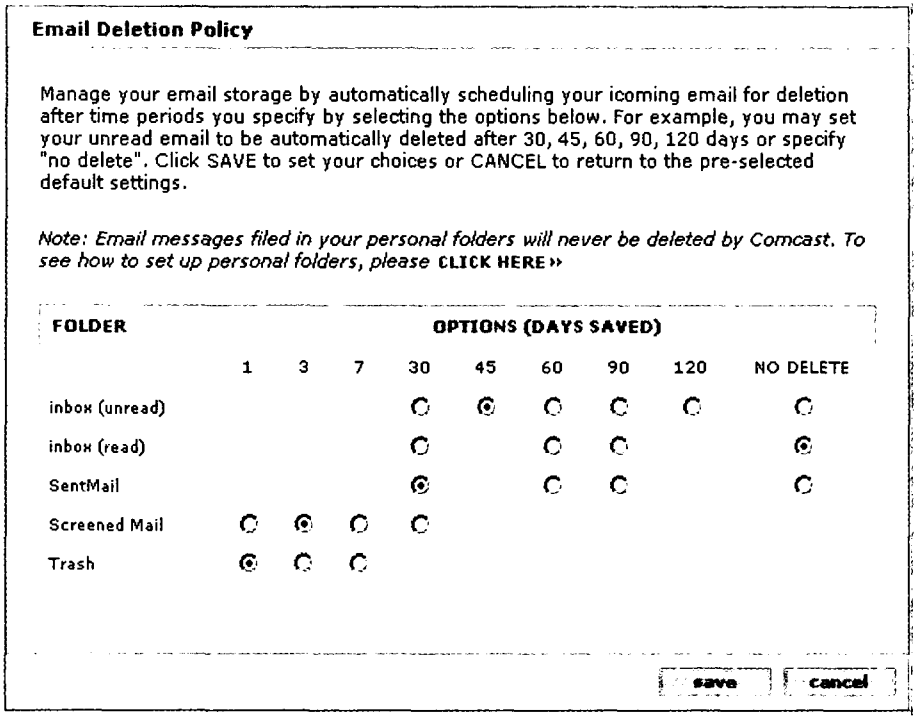
[31] Gmail was in beta at the time this study was undertaken.

Yahoo! Free	Termination - Inbox mail → 90 days from last activity Automatic deletion - Bulk folder mail → default is to delete every 30 days, however user can change this to a shorter period of time	Immediately (within a few minutes)	Fax death certificate to close the account Information in the account is non-transferable	Notify subscriber whose information is being sought. Release information after 15 days	Implies no
Yahoo! Paid	Termination - Inbox mail → 6 months from date of missed payment Automatic deletion - Bulk folder mail → default is every 30 days, however user can shorten time period	Immediately	Fax death certificate to close account Information in the account is non-transferable	Notify subscriber whose information is being sought Release information after 15 days (need to confirm)	Implies no
AOL	Termination - General account deleted after 4 months from last payment Automatic deletion - Unread (i.e., unopened) and sent email → 27 days Read email → about 3 days, and the user can extend this preference for up to 7 days	Read email→ immediately Deleted email→ 24 hours	Show death certificate and official proof that you are executor/ administrator of estate.	Notify subscriber promptly after subpoena is received. Release information after 2 weeks	Explicitly states no
Earthlink	Termination	Immediately	Accepts a death certificate or other legal documents proving authorization.	Notify customers after receiving civil request. Release information after minimum of 10 days	Unclear in written policy but public statements explicitly state no

Comcast	Termination - Email in primary account typically deleted within 90 days of account being marked for suspension and deletion due to termination of service.	Email removed from mail server within 24 hours of being deleted by subscriber; subscriber can immediately remove email from mail server by emptying webmail "trash." Note: certain configurable POP3 email clients may permit subscribers to override these rules.	Provide valid death certificate and proof of next of kin status.	Do not provide information in response to a standard civil subpoena; require court order. Upon receipt of valid court order, promptly give notice to subscriber. Current policy is to give customer 14 days notice prior to disclosing requested customer information.	Explicitly states no
Verizon (.Net and Domain based email services)	Termination - Mailbox closed after 6 months of being "unused" Automatic deletion – Inbox → 30 days Spam Detector → 7 days	Immediately	Send death certificate and provide general account information	Notify subscriber promptly after subpoena is received. Release information after 2 weeks	Implies no

* Assuming that it is a non-emergency situation.
** With exceptions for security purposes, etc.

Some providers are explicit about giving users notice and control over deletion/storage practices. For example, Comcast permits users to set their own email deletion timeframes for webmail folders. Copied below is the table of choices provided to subscribers, with the default settings checked. Other ISPs may also provide user-defined deletion policies for their webmail services.



Email Deletion Policy

Manage your email storage by automatically scheduling your icoming email for deletion after time periods you specify by selecting the options below. For example, you may set your unread email to be automatically deleted after 30, 45, 60, 90, 120 days or specify "no delete". Click SAVE to set your choices or CANCEL to return to the pre-selected default settings.

Note: Email messages filed in your personal folders will never be deleted by Comcast. To see how to set up personal folders, please **CLICK HERE »**

FOLDER	OPTIONS (DAYS SAVED)								
	1	3	7	30	45	60	90	120	NO DELETE
inbox (unread)				○	◉	○	○	○	○
inbox (read)				○		○	○		◉
SentMail				◉		○	○		○
Screened Mail	○	◉	○	○					
Trash	◉	○	○						

save cancel

Industry practices on retention and deletion vary, which is not a problem and may actually offer consumers desirable choices, so long as policies are clear. Policies range from defaults to user control. Emails from terminated free accounts, which are deleted based on date of last activity, generally seem to be deleted earlier than those in paid accounts, which are removed based on date of missed payment. For the most part, emails deleted by the customer are removed from the provider's server quickly, between a few hours to 3 days after the user has deleted them. Google's Gmail service does not specify a server removal date, but that seems to be due to extra precision on the part of the drafters of Google's privacy statement, recognizing that even when mail has been deleted from the ISP's server it may still be available for forensic discovery until it has been overwritten.

There is also a variety of policies with respect to next of kin requests. Most service providers require high levels of proof, such as death certificates, in order to verify next of kin requests. It is interesting to note that, even with documentation, Yahoo! does not give relatives access to the contents of a deceased person's account.

It is also interesting to see consistency in the way major ISPs handle civil subpoena requests. In non-emergency situations, every ISP we surveyed gives its customers notice soon after receiving subpoena requests, and then allows customers generally about two weeks to challenge the order prior to releasing information. (We assume that this practice applies to disclosure of both email content and subscriber identifying information.) Under the Cable Act, cable ISPs require a court order to disclose information to private parties and must provide notice to the subscriber, giving the subscriber an opportunity to object.

Most ISPs in our survey implied that they do not read their customers' email. Policies were not always explicit. As the *Councilman* case illustrated, there may be outliers among smaller ISPs.

POLICY RECOMMENDATIONS

Given the dramatic changes in technology, especially the shift to Web-based email and the offering of huge amounts of online storage, changes are needed in several areas. In particular, protecting user privacy calls for a mix of user education, industry policies to protect stored electronic communications better, and revisions to ECPA and other pertinent privacy laws.

Most of our suggested legal changes relate to government access. Some distinctions in ECPA now seem outdated. It no longer makes sense to provide different protections depending on how old an email is, or based on the possible (but disputed) distinction between opened versus unopened email. In 1986, when ECPA was adopted, downloaded email was generally not saved on the service providers' computers. Downloaded email, whether opened or unopened, usually sat only on the user's computer and was fully protected by the Fourth Amendment. Today, most corporate email still works that way, so that email is still kept on users' computers (including corporate back-up computers), not on Web servers or mail servers of third parties. However, in contrast to 1986, with regard to the significant percentage of email that is Web-based (including most consumer systems like AOL, Hotmail, Gmail, and YahooMail), opened email is commonly kept on third party servers. It is no longer sensible to accord it lower

protection. Accordingly, legislators should update the Electronic Communications Privacy Act to keep pace with these changes in technology. We recommend that ECPA be amended to provide, as a general rule, that the government not be able to obtain email content information without a search warrant. The "180 day" distinction and any distinction between opened and unopened email should be removed in light of the fact that, with Web-based email programs, open email is routinely kept on third party servers.[32] Similarly, the distinction between "electronic communications service providers" and "providers of remote computing service" should be eliminated – most ISPs are both, and most email moves from one to the other without the customer being aware that its legal status has changed.

The recent *Councilman* decision highlights a loophole in ECPA that technically allows service providers to read and use (but not disclose to others) the content of their subscribers' email. The company whose practices were at issue in *Councilman* may have been one of a kind. There is no evidence that other ISPs "read" customer emails. While major ISPs do not engage in this type of behavior, a narrowly-tailored reform would solidify customer confidence by making it clear that ISPs may only access subscribers' emails as required to provide the service, protect the ISPs rights or property, or in other limited circumstances.[33]

In the 108th Congress (2003-04), legislation was introduced to address some of these issues. The Email Privacy Act, sponsored in the House by Representative Inslee (D-WA), would have ensured that law enforcement officials have to obtain a wiretap order to gain real-time access to Internet communications. The Inslee bill also would have prevented ISPs from reading their customer's email except in cases where it is necessary to provide service or with consent. With the same intent, Representative Nadler (D-NY) introduced the Email Privacy Protection Act. However, while both bills would have helped to close the loophole highlighted by the *Councilman* decision, they did not address other shortcomings of ECPA.

It might also be desirable to have legislation addressing the rights and obligations of ISPs served with civil subpoenas. ECPA currently

---

[32] More information on CDT's position on the *Councilman* case can be found in CDT Policy Post 10.13, *supra* note 22.

[33] One way to accomplish this would be to add to the end of 18 U.S.C. § 2701(c)(1) (2002), the language in 18 U.S.C. § 2702(b)(5) (2002): "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service." This is essentially identical to the language applicable to telephone companies. *See* 18 U.S.C. § 2511(2)(a)(i) (2002).

prohibits ISPs from disclosing the email of their subscribers without some legal process, but it does not prohibit them from disclosing identifying information or transactional records to private parties. This should be addressed, by requiring at least a subpoena for disclosure of subscriber identifying information and transactional data. In addition, even though major ISPs, as a matter of policy, give notice to their subscribers when information is subpoenaed, it should be codified. It should also be made clear that notice must be given whether the subpoena is for content or identifying of transactional information. Legislation should place the responsibility for providing notice to the individual whose information is sought on the party requesting the subpoena unless that party does not know the subscriber's address, in which case the ISP should afford notice. The law should provide adequate time for the subscriber to contest the subpoena prior to the information being released. It should also require that the party requesting the subpoena provide the subscriber, or the ISP to pass on to the subscriber, sufficient information to understand the charges and the court in which they are being sued. The consensus standard found in our study, immediate notification and a 14-day waiting period prior to disclosure, is a starting point for such legislation.[34] Likewise, legislation should provide ISPs with the right to recover their reasonable costs incurred in processing and replying to private and government requests for customer information, whether resulting in a positive or negative response.

Termination and deletion questions do not require legislation. As a matter of industry practice, each ISP should clearly communicate to customers what its termination and deletion policies are. These policies should be available on their Web sites and in terms of service and privacy policies. A good practice may be to give users control, allowing them to set retention periods.

Much of the "next of kin" access problem stems from the fact that identifying information is relatively easy to obtain, so ISPs feel compelled to require people claiming to be relatives to provide high levels of authentication in order to prove their relation to the account holder and their need to access the account. One solution is for users to leave a copy of their passwords with relatives, but this too raises privacy and security issues. Clarification of policies regarding deletion times may help the situation by making it easier for consumers to realize how quickly they need to process next of kin

---

[34] In California, such an obligation may already exist as a matter of state privacy law. In 2003, legislation was introduced to codify the obligation, but did not pass. *See* The Internet Communications Protection Act, A.B. 1143, *supra* note 26.

requests. The thorny questions about privacy in the context of a deceased subscriber are worthy of further study. Industry should collaborate to develop appropriate and perhaps standardized practices in this area. One solution is for individuals to address this issue in their wills. Alternatively, ISPs could include in their terms of service some kind of standard language, similar to the beneficiaries clause in an insurance policy, stating that upon death of the subscriber stored data would be provided to designated persons.

The move to greater storage is certain to bring with it an even wider set of policy issues in the future, but addressing those in front of us is becoming more urgent as the email providers increase their capacity and services.